

Application No.: 09/777,550  
Amendment dated: August 6, 2004  
Reply to Office Action of 04-20-04  
Attorney Docket No.:0016.0006US1

c.) Remarks

Claims 1-34 and 36-48 are pending in this application. Claims 17, 21, 34, 36, and 37 have been amended. Claim 35 has been cancelled.

The specification was objected to for a specific informality. This has been corrected in the foregoing amendments. Further, the specification has been generally proofread and a number of grammatical corrections made.

Turning now to the merits, claims 1-48 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,321,338 to Porras, *et al.* (hereinafter Porras patent). This rejection is respectfully traversed for the following reasons.

Generally, the Porras patent is directed to a network surveillance method. Beginning at approximately column 7 of the specification, it describes signature engines that map an event stream against an abstract representation of event sequences that are known to indicate undesirable activity. In this way, it can scan streams of network activity to determine whether that activity is indicative of known attacks against the network. Specifically, at column 7, line 42, the Porras patent notes that the signature engines can detect address spoofing.

On a somewhat related vein, claim 1, for example, is directed to a network comprising network nodes and routing devices. Most relevantly, it comprises a director that determines "whether selected instances of source addresses of packets are spoof source addresses." According to the invention, however, and in contrast to the Porras patent, this determination is based at least in part on one or more consistency measures. Claim 15 has similar requirements. Claim 34 is directed to determining whether at least some instances of the source addresses are spoof instances based on spatial distribution of the addresses.

In short, with respect to claims 1 and 15, the present invention describes a method for using consistency measures to determine whether or not addresses are being spoofed, and claim 34 includes spatial distribution analysis.

Application No.: 09/777,550  
Amendment dated: August 6, 2004  
Reply to Office Action of 04-20-04  
Attorney Docket No.:0016.0006US1

Applicants respectfully believe that these claims are not anticipated by the Porras patent. Specifically, as noted, the most relevant section of Porras appears to be column 7, which indeed mentions address spoofing. Here, however, this spoofing is determined by reference to signature engines that "scan" the event stream for events that represent attempted exploitations of known attacks against the service. On contrast, the present claimed invention uses consistency measures or address spatial distribution.

In short, the Porras patent does not disclose to detect address spoofing by using consistency measures as claimed.

Thus, there is no anticipation.

Applicants believe that the present application is in condition for allowance. A Notice of Allowance is respectfully solicited. Should any questions arise, the Examiner is encouraged to contact the undersigned.

Respectfully submitted,

By 

J. Grant Houston  
Registration No.: 35,900  
Tel.: 781 863 9991  
Fax: 781 863 9931

Lexington, Massachusetts 02421  
Date: August 6, 2004